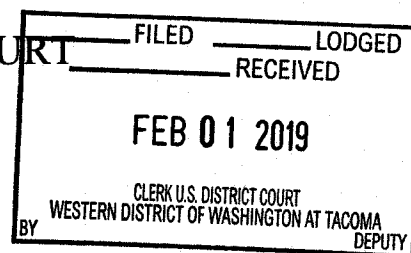


UNITED STATES DISTRICT COURT

for the

Western District of Washington



In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)8601 NE 36th Street, Vancouver, Washington 98662,
more fully described in Attachment A

Case No.

MJ19-5015

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

8601 NE 36th Street, Vancouver, Washington 98662, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

26 U.S.C. § 7201

26 U.S.C. § 7206(2)

Offense Description

Tax Evasion

Preparation of False Tax Returns

The application is based on these facts:

- ☒ See Affidavit of Christian Martin, continued on the attached sheet.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Christian D. Martin

Applicant's signature

Christian D. Martin, Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 02/01/2019

J. Richard Creatura

Judge's signature

City and state: Tacoma, Washington

J. Richard Creatura, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Christian D. Martin, being first duly sworn on oath, depose and say:

AFFIANT BACKGROUND

1. I am a Special Agent with the Internal Revenue Service (IRS) and have been since September 2001. My current assignment is to conduct and assist in investigations of various white collar crimes including tax fraud, tax-related fraud, and identity theft. My training and experience includes completion of the basic training requirements for a Special Agent at the Federal Law Enforcement Training Center and participation in numerous investigations, during the course of which I have interviewed suspects and witnesses, executed court-authorized search and arrest warrants, and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement.

2. Facts in this affidavit are based on my personal knowledge, my training and experience, and information I have gathered from other law enforcement personnel, witnesses, and documents obtained during the course of the investigation. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not include each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are relevant to the determination of probable cause to support the issuance of the requested warrant.

PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 8601 NE 36th Street, Vancouver, Washington 98662 (hereinafter referred to as the "PREMISES" and more particularly described in Attachment A to that application and

1 incorporated by reference herein) for documents, records, electronic media and other
2 items (more particularly described in Attachment B to that application and incorporated
3 by reference herein) which constitute evidence of the commission of criminal offenses,
4 fruits of those offenses, and property designed or intended for use or which has been used
5 as the means of committing criminal offenses, that is, evasion of the payment of personal
6 and corporate taxes, in violation of Title 26, United States Code, Section 7201; and
7 willful aiding or assisting in the preparation of false tax returns, in violation of Title 26,
8 United States Code, Section 7206(2).

9 **APPLICABLE LAW**

10 4. Title 26, United States Code, Section 7201 provides that whoever willfully
11 attempts in any manner to evade or defeat any tax imposed by this title or the payment
12 thereof shall, in addition to other penalties provided by law, be guilty of a felony and,
13 upon conviction thereof, shall be fined not more than \$250,000 (\$500,000 in the case of a
14 corporation), or imprisoned not more than 5 years, or both, together with the costs of
15 prosecution.

16 5. Title 26, United States Code, Section 7206(2) provides that whoever
17 willfully aids or assists in, or procures, counsels, or advises the preparation or
18 presentation under, or in connection with any matter arising under, the internal revenue
19 laws, of a return, affidavit, claim, or other document, which is fraudulent or is false as to
20 any material matter, whether or not such falsity or fraud is with the knowledge or consent
21 of the person authorized or required to present such return, affidavit, claim, or document
22 shall, in addition to other penalties provided by law, be guilty of a felony and, upon
23 conviction thereof, shall be fined not more than \$100,000 (\$500,000 in the case of a
24 corporation), or imprisoned not more than 3 years, or both, together with the costs of
25 prosecution.

26 **SUMMARY OF INVESTIGATION**

27 6. This investigation concerns Conexión Latina, a business providing
28 immigration and accounting services to Vancouver's Hispanic community. Conexión

1 Latina is operated by SAUL VALDEZ and his mother, Abby Eden-Albrecht, at the
2 PREMISES. Conexion Latina has a business website, the address of which is
3 conexionalatinapdx.com, which lists the PREMISES as the business location under the
4 section "Contact us." The website also includes biographies for its two "Public
5 Notaries," Albrecht and VALDEZ, and lists VALDEZ as the company's CEO. The
6 "Services" page of the website includes a list of services provided by the company, which
7 includes "Accounting" and, specifically "personal taxes." Additionally, on the Conexion
8 Latina homepage is the statement, "We will get the maximum possible refund!"

9 7. On November 16, 2018, I received a referral from the Return Preparer
10 Program coordinator of the IRS Criminal Investigation Division's Seattle Field office.
11 The referral, which originated with the Scheme Development Center (SDC),¹ alleges that
12 VALDEZ, doing business as Conexion Latina, is preparing false federal income tax
13 returns. Specifically, the referral alleges that VALDEZ is preparing returns that contain
14 questionable Schedule A itemized deductions including unreimbursed employee business
15 expenses (UEBEs) and legal fees. UEBEs are miscellaneous itemized deductions (MIDs)
16 that can be deducted by employees on their respective Schedules A attached to their Form
17 1040. UEBEs must be (1) paid or incurred during the year, for carrying on your trade or
18 business of being an employee, and (2) ordinary and necessary. Additionally, MIDs are
19 subject to a two percent (2%) limit, and the deduction is calculated by adding together all
20 MIDs and subtracting two percent (2%) of one's adjusted gross income. It is particularly
21 important to note that expenses for commuting, or driving to work from home and vice
22 versa, are not deductible as UEBE, and neither are uniforms, unless the uniforms are
23 required as a condition of employment *and* not suitable for everyday wear. Legal fees are
24 deductible if the expense is incurred attempting to produce or collect taxable income or
25 paid in connection with the determination, collection, or refund of any tax.

26 _____
27 ¹ The Scheme Development Center (SDC) reviews and analyzes tax returns to detect fraudulent
28 refund schemes.

8. The SDC referral also indicated that VALDEZ did not sign any of the returns as the paid preparer. When a third-party tax preparer creates and files a tax return on behalf of a taxpayer, he is required by law to list on the return his name or tax-preparation firm's name, as well as his phone number and address. A tax preparer is also required to list on the return his Preparer Tax Identification Number² (PTIN) and/or his firm's employer identification number (EIN). In my experience and expertise with other schemes in which tax preparers have defrauded a taxpayer or the federal government, I am aware that the tax preparer often does not provide this identifying information on the return. By failing to provide identifying information, the tax preparer attempts to evade detection and liability for false information that may be set out in the return.

9. Because VALDEZ did not sign any of the returns, the SDC could not simply search tax returns for VALDEZ's identifying information. Instead, the SDC attempted to identify the returns that had been prepared by VALDEZ on the basis of other information; specifically: (a) the email addresses associated with electronically-submitted tax returns;³ (b) the IP addresses associated with electronically-submitted tax returns;⁴ and (c) the Device Identification number (Device ID) associated with the electronically-submitted tax returns.⁵ The SDC found 2,845 federal income tax returns

² Anyone who prepares or assists in preparing federal tax returns for compensation must have a valid PTIN before preparing returns.

³ When electronically submitting a Federal Income Tax return to the IRS, taxpayers and preparers have the option to input an email address so that they may receive notifications about their returns via email.

⁴ An IP address is a unique numerical label assigned to a device, like a computer or wireless router, participating in a computer network that uses IP for communication. An IP address serves two principal functions: interface identification and location addressing. IP addresses can be used to track internet usage to a particular Internet Service Provider customer.

⁵ The IRS implemented a Device ID field for electronic return filers and preparers for processing year 2015. The Device ID should contain unique data, accessed and transmitted by the software used to create the electronic return, which will identify the specific computer from which the tax return was electronically filed. The Device ID field was voluntary for processing year 2015 but became mandatory for processing year 2016.

1 for the tax year 2017 that shared one or more of these criteria with email addresses, IP
 2 addresses, or Device IDs associated with VALDEZ or Conexion Latina. Of these
 3 2,845 returns, ninety-four percent (94%) claimed refunds and forty-six percent (46%)
 4 claimed UEBEs. The national averages for 2017 federal income tax returns include
 5 eighty-two percent (82%) that claim refunds and ten percent (10%) that claim UEBEs, so
 6 the returns believed to have been prepared by VALDEZ and Conexion Latina are
 7 significantly above the national averages.

8 10. As previously mentioned, one of the identifiers searched by the SDC in
 9 determining which returns were prepared by VALDEZ was email address. An email
 10 address is composed of three parts: the local-part, which comes at the beginning; an @
 11 symbol, which comes immediately after the local-part; and the domain. The domain
 12 name for Conexion Latina's website is conexionlatinapdx.com. Of the 2,845 returns
 13 identified by the SDC as having been prepared by VALDEZ, 1,449 were submitted with
 14 an email address that contained "conexionlatinapdx" either in the local-part or the
 15 domain. Forty four additional returns were submitted with an email address that
 16 contained "conexionlatina" in the local-part, and numerous other submitted returns
 17 contained variations of the name SAUL VALDEZ, including saulvaldezusa@gmail.com.

18 11. Conexion Latina was assigned EIN 81-3600183 by the IRS in August 2016
 19 and is listed as a single member limited liability company with VALDEZ being the single
 20 member. VALDEZ filed his 2015 and 2016 Forms 1040 in December 2017 and reported
 21 the income and expenses for Conexion Latina on a Schedule C attached to each Form
 22 1040. VALDEZ's 2017 Form 1040 was due to be filed by April 17, 2018 but has yet to
 23 be filed. Additionally, no 2017 return has been filed for Conexion Latina.

24 Client Interviews

25 12. After the SDC discovered the tax returns prepared and filed by VALDEZ, I
 26 selected four of his clients to interview. All four clients had their returns prepared by
 27 VALDEZ in 2018. Additionally, all four clients filed 2017 federal income tax returns
 28 with questionable UEBEs and legal expenses. The expenses are questionable because

1 they are not typical for the clients' stated occupations and they do not appear to be
2 specific to the client. For instance, three of the clients' returns contain a parking expense
3 of \$2,100 and the fourth contains a parking expense of \$2,101. Two clients' returns
4 contain a legal expense of \$1,500 and the other two contain a legal expense of \$2,500.
5 Two clients even had the exact same vehicle information on their respective forms: a
6 placed-in-service date of 02/01/2017; total miles driven of 13,559; business miles of
7 9,051; commuting distance of 15 miles; and commuting miles of 1,200.

8 13. On January 4, 2019, I interviewed a witness referred to herein as "MC."
9 MC was shown the Washington Department of Licensing photo of VALDEZ, and MC
10 confirmed that VALDEZ prepared MC's 2017 Form 1040. MC was shown a picture of
11 the PREMISES and confirmed that VALDEZ prepared MC's return in an office within
12 the PREMISES. MC met VALDEZ at the PREMISES and sat with VALDEZ in his
13 office while he prepared MC's return on a desktop computer. Upon completion,
14 VALDEZ printed a copy of MC's return and manually completed the "Paid Preparer Use
15 Only" section. In this section, VALDEZ printed and signed his name and printed the
16 name, address, phone number, and EIN of the business along with his PTIN and the date,
17 August 10, 2018. MC allowed me to review and make a copy of MC's return. The "Paid
18 Preparer Use Only" section on the electronically filed return, however, is blank. The
19 electronically filed return was transmitted to the IRS on August 10, 2018. MC paid
20 VALDEZ between \$150 and \$200 for his service.

21 a. MC's filed 2017 Form 1040 contains an expense of \$2,500 for legal
22 fees on line 23 of the Schedule A, but MC stated that he/she did not provide this
23 expense to VALDEZ or discuss it with VALDEZ.

24 b. MC's return also contains an expense of \$3,242 (\$1,141 for MC and
25 \$2,101 for MC's spouse) for parking fees, tolls and transportation included in the
26 total on line 21 of the Schedule A. MC stated that he/she did not provide this
27 expense to VALDEZ or discuss it with VALDEZ.
28

1 14. On January 8, 2019, I interviewed a witness referred to herein as "MR."
2 MR was shown the Washington Department of Licensing photo of VALDEZ, and MR
3 confirmed that VALDEZ prepared MR's 2017 Form 1040. MR was shown a picture of
4 the PREMISES and confirmed that VALDEZ prepared MR's return in an office within
5 the PREMISES. MR said that VALDEZ's office is just inside and to the right of the
6 front door of the PREMISES. MR paid VALDEZ approximately \$90 cash for his
7 service. MR met VALDEZ at the PREMISES and sat with VALDEZ in his office while
8 he prepared MR's return on a desktop computer. MR said VALDEZ gave MR a copy of
9 the return, but MR could not find it for the interview. MR's 2017 Form 1040 was
10 electronically transmitted to the IRS on May 14, 2018.

11 a. MR's filed 2017 Form 1040 contains an expense of \$1,500 for legal
12 fees on line 23 of the Schedule A. MR stated that he/she incurred approximately
13 \$3,000 in legal fees in 2017 related to a DUI. MR also stated that VALDEZ asked
14 if MR paid legal fees in 2017, but did not ask if the legal fees were related to
15 income or taxes.

16 b. MR's return also contains an expense of \$2,100 for parking fees,
17 tolls and transportation included in the total on line 21 of the Schedule A. MR
18 pays between \$2 and \$5 to park at work, and MR told investigators that VALDEZ
19 calculated the parking expense based on that dollar range and the number of days
20 MR worked. MR did not provide VALDEZ with any parking receipts, and MR
21 was not informed by VALDEZ that fees paid to park a car at work are
22 nondeductible commuting expenses.

23 c. MR's return contains a vehicle expense of \$5,837 included in the
24 total on line 21 of the Schedule A. According to MR, this expense was calculated
25 by multiplying 10,910 miles by the standard mileage rate of \$.535. Driving is not,
26 however, one of MR's work duties. MR said that VALDEZ asked MR how far
27 MR's commute was, but MR did not know, so VALDEZ used Google Maps to
28 calculate the distance at 50 miles, and then multiplied that number by the

1 approximate number of shifts that MR worked. MR was not informed by
2 VALDEZ that commuting is not deductible.

3 d. MR's return also contains a meals and entertainment expense of
4 \$2,544 included in the total on line 21 of the Schedule A. MR works as a waiter in
5 a restaurant and sometimes buys meals during shifts. MR does not conduct a trade
6 or business and, therefore, does not have deductible business-related meals or
7 entertainment. VALDEZ did not inform MR that MR's meals were a
8 nondeductible personal expense.

9 e. MR's return contains a tools and supplies expense of \$957 included
10 in the total on line 21 of the Schedule A. MR stated that he/she did not incur this
11 expense and did not provide it to VALDEZ.

12 f. Lastly, MR's return contains an expense for uniforms of \$1,190
13 included in the total on line 21 of the Schedule A. MR did have to buy black
14 pants, black shirts, and slip-resistant black shoes for work, but MR said that these
15 items cost only approximately \$300. MR did not provide VALDEZ with the
16 \$1,190 figure. Also, the clothes MR wears for work appear to be suitable for
17 everyday wear and, therefore, would not be a deductible expense. VALDEZ did
18 not inform MR of the rules for these requirements for the deduction.

19 15. My original intent when arriving at MR's home was to interview MR's
20 child, referred to herein as "JL," who's 2017 Form 1040 was also prepared by VALDEZ.
21 MR said that JL had moved away, but that MR could answer any questions I had because
22 MR was the one who had JL's return prepared by VALDEZ. MR said JL was a college
23 student in 2017 and worked part-time in retail. MR confirmed that VALDEZ prepared
24 JL's 2017 Form 1040 at the PREMISES. MR paid VALDEZ \$190 in cash to prepare
25 JL's 2017 Form 1040. JL's 2017 Form 1040 contained the following questionable
26 expenses: legal fees of \$1,500 on line 23 of the Schedule A; a vehicle expense of \$4,842
27 included in the total on line 21 of the Schedule A; a parking expense of \$2,100 included
28 in the total on line 21 of the Schedule A; and meals of \$586 included in the total on line

21 of the Schedule A. MR immediately recognized that JL's legal fees and parking expenses were the same as those deducted in MR's 2017 Form 1040. MR said JL did not incur any of these expenses and MR did not provide these expenses to VALDEZ. MR provided me with a copy of JL's 2017 Form 1040, which MR made from the copy provided by VALDEZ. The "Paid preparer use only" section is blank. JL's return was electronically transmitted to the IRS on August 28, 2018.

16. On January 9, 2019, I interviewed a witness referred to herein as "BR." BR was shown the Washington Department of Licensing photo of VALDEZ, and BR confirmed that VALDEZ prepared BR's 2017 Form 1040A. BR was shown a picture of the PREMISES and confirmed that VALDEZ prepared BR's return in an office within the PREMISES. BR said VALDEZ's office is just inside and to the right of the front door of the PREMISES. BR paid VALDEZ \$204.63 via credit card to prepare BR's 2017 Form 1040A. BR allowed me to copy the payment receipt and BR's 2017 Form 1040A, received from VALDEZ. The payment receipt was originally emailed to saulvaldezusa@gmail.com and printed for BR by VALDEZ. The "Paid preparer use only" section of BR's copy is blank. BR met VALDEZ at the PREMISES and sat with VALDEZ in his office while he prepared BR's 2017 Form 1040A on a desktop computer. Prior to meeting with VALDEZ, BR used TurboTax online to prepare his/her 2017 Form 1040A, but did not file it. BR said the refund due on the TurboTax version was approximately \$500 less than the refund calculated by VALDEZ, but BR no longer had access to the file to show me. BR said VALDEZ asked few questions while preparing BR's 2017 Form 1040A. BR's filed 2017 Form 1040A contains an education credit of \$718 on line 33, which is based on education expenses of \$3,430. BR's Form 1098-T,⁶ which BR received from Clark College, shows qualified tuition expenses of only \$550.55. BR confirmed that he/she provided the Form 1098-T to VALDEZ, that the

⁶ The Form 1098-T is prepared by eligible colleges and/or post-secondary schools for each student who paid qualified educational expenses. The Form 1098-T reports, among other things, the total amount of qualifying educational expenses either paid by or billed to the student.

1 \$550.55 was all that BR had paid for education expenses in 2017, and that he/she did not
2 provide VALDEZ with the expense of \$3,430. BR's return was electronically
3 transmitted to the IRS on August 23, 2018.

4 17. On January 9, 2019, Special Agent (SA) Jason Nix and I interviewed a
5 witness referred to herein as "MM." MM does not speak fluent English and SA Nix
6 served as an interpreter. MM was shown the Washington Department of Licensing photo
7 of VALDEZ, and MM confirmed that VALDEZ prepared MM's 2017 Form 1040. MM
8 was shown a picture of the PREMISES and confirmed that VALDEZ prepared MM's
9 return in an office within the PREMISES. MM paid VALDEZ \$195 via credit card for
10 his service, and MM provided me with the receipt, which I copied. The receipt was
11 originally emailed to saulvaldezusa@gmail.com and printed for MM by VALDEZ. MM
12 met VALDEZ at the PREMISES and sat with VALDEZ in his office while he prepared
13 MM's return on a desktop computer. Upon completion, VALDEZ printed a copy of
14 MM's return and completed the "Paid Preparer Use Only" section. In this section,
15 VALDEZ printed and signed his name and printed the name, address, phone number, and
16 EIN of the business, along with his PTIN. The "Paid Preparer Use Only" section on the
17 filed return is blank. MM's return was electronically transmitted to the IRS on
18 September 19, 2018.

19 a. MM's filed 2017 Form 1040 contains an expense of \$2,500 for legal
20 fees on line 23 of the Schedule A. MM did not provide this expense to VALDEZ.

21 b. MM's 2017 Form 1040 also contains the following UEBE's on line
22 21 of the Schedule A: a vehicle expense of \$4,842; parking of \$2,100; meals and
23 entertainment of \$958; tools and supplies of \$990; and uniforms of \$871. MM
24 said that the only expense he/she provided to VALDEZ was for uniforms, but that
25 the amount he/she provided was much less than what is reported on the return.
26 Moreover, the pants and slip-resistant shoes that MM purchased for work appear
27 to be suitable for everyday wear and, therefore, would not be a deductible expense.

28 In addition, VALDEZ did not collect information from MM to support the vehicle

1 and parking expenses submitted in the return. MM works in restaurants as a food
2 preparer and had to drive to other locations on 2 or 3 occasions to pick up
3 supplies, but VALDEZ never asked about these expenses. MM otherwise did not
4 operate a vehicle for work except for commuting.

5 **Description of the PREMISES**

6 18. The PREMISES is a small house located in a residential neighborhood.
7 County property records list Albrecht as the property owner. Clark Public Utilities
8 provides electric service for the PREMISES and the name on the account is Conexion
9 Latina. The City of Vancouver provides other utilities, including water and sewage, for
10 the PREMISES, and the name on that account is Conexion Latina. Conexion Latina is
11 registered with the Washington Secretary of State and the PREMISES is listed as the
12 principal office street address. A sign affixed to the front door displays the Conexion
13 Latina name and logo along with the business hours, address, and phone numbers for
14 Albrecht, VALDEZ, and the office.

15 19. Surveillance of the PREMISES has been conducted on numerous occasions
16 during January 2019. Albrecht has been observed greeting clients at the entrance to the
17 PREMISES on several occasions, and a white Jeep Wrangler registered to Albrecht has
18 been seen parked in the front driveway of the PREMISES on all but one occasion.
19 VALDEZ has been observed working in his office at the front of the PREMISES and
20 greeting customers at the PREMISES' entrance on several occasions, and a dark-colored
21 Range Rover registered to VALDEZ has been observed on a parking strip directly east of
22 the PREMISES on all but one occasion.

23 20. Despite being located in a residential area, nothing observed during
24 surveillance indicates that the PREMISES is used as a residence. Albrecht and VALDEZ
25 each have homes separate from the PREMISES. Albrecht lives in Vancouver, WA, and
26 VALDEZ lives in Portland, OR. On several occasions both Albrecht's and VALDEZ's
27 registered vehicles, the Jeep and Range Rover, have been observed parked at their
28 respective homes prior to later being observed arriving at the PREMISES. City of

1 Vancouver code enforcement records indicate that an inspection was conducted on the
2 PREMISES in March 2018 and again in April 2018 after one or more complaints were
3 received about a business being conducted at the PREMISES. The inspector indicated
4 that numerous customers were at the PREMISES during each inspection and that no one
5 was actually residing at the PREMISES.

6 **SUMMARY OF PROBABLE CAUSE**

7 21. Based on my training and experience, persons engaged in tax schemes,
8 conspiracies to defraud the United States, evasion of income tax, the filing of false
9 returns, and obstruction of the administration of the income tax law often maintain
10 records for long periods of time, particularly when they are involved in a pattern of
11 conduct over a long period of time. There are many reasons why criminal offenders
12 maintain evidence for long periods of time. The evidence may be innocuous at first
13 glance (e.g. financial, credit card and banking documents, travel documents, receipts,
14 documents reflecting purchases of assets, personal calendars, telephone and address
15 directories, check books, videotapes and photographs, utility records, ownership records,
16 letters and notes, tax returns and financial records, escrow files, telephone and pager bills,
17 keys to safe deposit boxes, packaging materials, computer hardware and software), but
18 have significance and relevance when considered in light of other evidence. The criminal
19 offender may no longer realize he still possesses the evidence or may believe law
20 enforcement could not obtain a search warrant to seize the evidence. The criminal
21 offender may also be under the mistaken belief that he/she has deleted, hidden or further
22 destroyed any computer-related evidence, which may be retrievable by a trained forensic
23 computer expert. In addition, 26 United States Code § 6001 and the corresponding
24 regulations require taxpayers keep records for no less than three years after the return is
25 filed.

26 22. Based on my training and experience, persons engaged in tax schemes,
27 conspiracies to defraud the United States, evasion of income tax, the filing of false
28 returns, and obstruction of the administration of the income tax law, frequently retain

1 records of their correspondence and transactions within their business and other places
2 under their control. These records may be in the form of written communications,
3 emails, receipts, negotiated instruments, contracts, bank statements, tax returns, and other
4 records. Records of this kind are often also stored on computer media.

5 23. Based on my training and experience, I know that companies often keep
6 their financial and business records where they conduct business. This allows the
7 company to consult and use the information when making business decisions and
8 preparing financial information, including for legal and regulatory purposes such as filing
9 tax returns. Other such documents kept by companies include:

- 10 a. Banking records, such as bank statements, cancelled checks, withdrawal
11 slips, check registers, deposit tickets, loan documents, and correspondence;
- 12 b. Income records, such as sales invoices, receipts, cash register tapes, cash
13 receipt logs, sales journals, credit card merchant account statements and
14 records, and customer information;
- 15 c. Expense records, such as purchase receipts, invoices, credit card statements,
16 copies of cashier's checks, petty cash logs, journals and ledgers of
17 expenditures;
- 18 d. Asset acquisition and disposal records, such as titles, deeds, contracts,
19 receipts, inventory records, invoices and depreciation schedules;
- 20 e. Payroll records, such as employee lists, time cards, Forms W-2, Forms W-
21 4, and records of payments;
- 22 f. Financial records, such as income statements, cash flow statements, balance
23 sheets, bookkeeping records, and income and expense projections;
- 24 g. Tax documents, such as filed and unfiled state and federal income and
25 excise tax returns and employment tax returns;
- 26 h. Audit and compliance records, such as correspondence with or about audits
27 and compliance requirements, copies of complete or incomplete financial
28 disclosure forms, including Form 8300;

i. Regulatory and industry association information, such as guides to best practices, industry training/conference materials, rules and regulations, business and other licenses, pamphlets/notices, regulatory and compliance requirements, and correspondence with regulatory agencies; and

j. Corporate records, such as incorporation records, annual reports, stock books/ownership records, agreements, and shareholder or investor loans.

Surveillance of the PREMISES, along with records obtained by agents and reviewed in the course of this investigation, demonstrates that VALDEZ conducts business at the PREMISES, as Conexion Latina.

24. Based on my training and experience, I also know that owners of small and closely held businesses often keep personal records and documents at their place of business. These records often include personal bank records, records showing asset ownership and acquisition, investments, records of cash hoards, insurance records, loan records, promissory notes, agreements, correspondence, travel documents, safe deposit box keys, notes, and tax information.

25. Based upon my training and experience, I know that individuals and businesses commonly use computers or other electronic storage media to prepare and store the records described above and to prepare, complete, print, and file tax returns. It is likely that the records described above would be found on computers and other electronic storage media found in the PREMISES for the following reasons:

a. Each client interviewed observed VALDEZ prepare his/her respective return on a computer in the PREMISES.

b. For each client interviewed, VALDEZ used a computer in the PREMISES to print a copy of his/her 2017 federal income tax return.

c. All returns identified and believed to be prepared by VALDEZ were transmitted to the IRS electronically from a computer. The IRS received a Device ID as part of each transmission, and each client interviewed stated that his/her return was submitted to the IRS electronically.

d. While conducting surveillance, I personally observed VALDEZ sitting at a desk in his office, working on a computer.

1 e. The website for Conexion Latina has a "Contact" page, which
 2 contains a "Contact by Email" form to be completed and submitted by clients for
 3 appointments. This same page also contains the following statement, "If you want
 4 to hire any of our services you must do it by making an appointment through our
 contact form, or through the telephone below."

5 26. Based on my training and experience, I know that these business and
 6 personal records kept where a company conducts business can be useful in showing
 7 whether a person or entity reported all income to the IRS or evaded federal tax
 8 requirements.

9 27. Based on my training and experience, when investigating tax crimes, I
 10 know that it is useful to compare tax and financial records maintained by a business over
 11 the course of multiple years in order to evaluate, among other things, the business'
 12 income, expenditures, and accounting practices. Based on my training and experience,
 13 companies retain business records for extended periods of time and are legally obligated
 14 to retain tax records for multiple years after a return is filed or tax is paid.

15 **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**⁷

16 28. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
 17 Rules of Criminal Procedure, the application for the PREMISES seeks authorization to
 18 seize, image, or otherwise copy digital devices or other electronic storage media that
 19 reasonably appear capable of containing some or all of the data or items that fall within
 20 the scope of Attachment B to this Affidavit, and will specifically authorize a later review
 21 of the media or information consistent with the warrant.

22
 23 ⁷ Based on my training and experience, I use the following technical terms to convey the
 following meanings:

24 a. *Internet*. The Internet is a global network of digital devices that communicate
 25 with each other. Due to the structure of the Internet, connections between devices on the Internet
 26 often cross state and international borders, even when the devices communicating with each
 other are in the same state.

27 b. *Storage medium*. A storage medium is any physical object upon which data can
 28 be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and
 other magnetic or optical media.

1 29. I submit that if a computer or storage medium is found at the PREMISES
2 there is probable cause to believe that evidence, fruits, and/or instrumentalities of crimes
3 – specifically, violations of 26 U.S.C. §§ 7201 & 7206(2) – will be stored on those
4 digital devices or other electronic storage medium, for at least the following reasons:

5 a. Based on actual inspection of evidence related to this investigation,
6 such as bank statements, financial statements and emails, I am aware that
7 computer equipment was used to generate, store, and print documents used in
8 filing tax returns that could violate 26 U.S.C. §§ 7201 and 7206(2). There is
9 reason to believe that there are computer systems currently located at the
10 PREMISES.

11 b. A review of evidence and witness statements shows that VALDEZ
12 prepared returns on a computer and printed client return copies from a computer.

13 c. Review of evidence in this investigation shows that VALDEZ used
14 the TaxAct software program to prepare and transmit tax returns to the IRS.

15 d. Review of evidence in this investigation shows that VALDEZ
16 entered email addresses, for accounts to which he had access to or it is reasonable
17 to believe he had access to, into the TaxAct software program to receive status
18 updates on the processing of returns.

19 e. Based on my knowledge, training, and experience, I know that
20 computer files or remnants of such files can be recovered months or even years
21 after they have been downloaded onto a storage medium, deleted, or viewed via
22 the Internet. Electronic files downloaded to a storage medium can be stored for
23 years at little or no cost. Even when files have been deleted, they can be recovered
24 months or years later using forensic tools. This is so because when a person
25 “deletes” a file on a computer, the data contained in the file does not actually
26 disappear; rather, that data remains on the storage medium until it is overwritten
27 by new data.

28 f. Therefore, deleted files, or remnants of deleted files, may reside in
free space or slack space—that is, in space on the storage medium that is not
currently being used by an active file—for long periods of time before they are
overwritten. In addition, a computer’s operating system may also keep a record of
deleted data in a “swap” or “recovery” file.

 g. Wholly apart from user-generated files, computer storage media—in
particular, computers’ internal hard drives—contain electronic evidence of how a
computer has been used, what it has been used for, and who has used it. To give a

1 few examples, this forensic evidence can take the form of operating system
2 configurations, artifacts from operating system or application operation; file
3 system data structures, and virtual memory "swap" or paging files. Computer
4 users typically do not erase or delete this evidence, because special software is
5 typically required for that task. However, it is technically possible to delete this
6 information.

7 h. Similarly, files that have been viewed via the Internet are sometimes
8 automatically downloaded into a temporary Internet directory or "cache."

9 30. As further described in Attachment B to the application for the PREMISES,
10 I am seeking permission to locate not only computer files that might serve as direct
11 evidence of the crimes described on the warrant, but also for forensic electronic evidence
12 that establishes how computers were used, the purpose of their use, who used them, and
13 when. There is probable cause to believe that this forensic electronic evidence will be on
14 any digital device in the PREMISES because, based on my knowledge, training and
15 experience, I know:

16 a. Data on the storage medium can provide evidence of a file that was
17 once on the storage medium but has since been deleted or edited, or of a deleted
18 portion of a file (such as a paragraph that has been deleted from a word processing
19 file). Virtual memory paging systems can leave traces of information on the
20 storage medium that show what tasks and processes were recently active. Web
21 browsers, e-mail programs, and chat programs store configuration information on
22 the storage medium that can reveal information such as online nicknames and
23 passwords. Operating systems can record additional information, such as the
24 attachment of peripherals, the attachment of USB flash storage devices or other
25 external storage media, and the times the computer was in use. Computer file
26 systems can record information about the dates files were created and the sequence
27 in which they were created, although this information can later be falsified.

28 b. Forensic evidence on a computer or storage medium can also
indicate who has used or controlled the computer or storage medium. This "user
attribution" evidence is analogous to the search for "indicia of occupancy" while
executing a search warrant at a residence. For example, registry information,
configuration files, user profiles, e-mail, e-mail address books, "chat," instant
messaging logs, photographs, the presence or absence of malware, and
correspondence (and the data associated with the foregoing, such as file creation
and last-accessed dates) may be evidence of who used or controlled the computer

1 or storage medium at a relevant time. Further, forensic evidence on a digital
2 device can show how and when it was accessed or used. Such "timeline"
3 information allows the forensic analyst and investigators to understand the
4 chronological context of access to the digital device, its use, and events relating to
5 the offense under investigation. This "timeline" information may tend to either
6 inculcate or exculpate the user of the digital device. Last, forensic evidence on a
7 digital device may provide relevant insight into the user's state of mind as it
8 relates to the offense under investigation. For example, information on a digital
9 device may indicate the user's motive and intent to commit a crime (e.g., relevant
10 web searches occurring before a crime indicating a plan to commit the same),
11 consciousness of guilt (e.g., running a "wiping program" to destroy evidence on
12 the digital device or password protecting or encrypting such evidence in an effort
13 to conceal it from law enforcement), or knowledge that certain information is
14 stored on a digital device (e.g., logs indicating that the incriminating information
15 was accessed with a particular program).

16 c. A person with appropriate familiarity with how a computer works
17 can, after examining this forensic evidence in its proper context, draw conclusions
18 about how computers were used, the purpose of their use, who used them, and
19 when.

20 d. The process of identifying the exact files, blocks, registry entries,
21 logs, or other forms of forensic evidence on storage medium that are necessary to
22 draw an accurate conclusion is a dynamic process. While it is possible to specify
23 in advance the records to be sought, computer evidence is not always data that can
24 be merely reviewed by a review team and passed along to investigators. Whether
25 data stored on a computer is evidence may depend on other information stored on
26 the computer and the application of knowledge about how a computer behaves.
27 Therefore, contextual information necessary to understand other evidence also
28 falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the
purpose of its use, who used it, and when, sometimes it is necessary to establish
that a particular thing is not present on a storage medium. For example, the
presence or absence of counter-forensic programs or anti-virus programs (and
associated data) may be relevant to establishing the user's intent.

31. I know that when an individual uses either a business or personal computer
in keeping records the individual's business computers often will serve both as
instrumentalities for committing the crime and storage media for evidence of the crime.

1 Based on the information in this Affidavit, I believe that the digital devices belonging to
2 VALDEZ and Conexion Latina at the PREMISES are instrumentalities of crime as well
3 as storage devices, because they constitute the means by which VALDEZ committed the
4 violations. Any personal or business computers belonging to VALDEZ or Conexion
5 Latina at the PREMISES likely were used to commit the crimes of evasion of assessment
6 and willful aiding or assisting in the preparation of false tax returns in violation of 26
7 U.S.C. §§ 7201 & 7206(2) because they were likely used by VALDEZ (a) to prepare
8 client tax returns; (b) collect payments for the business; (c) to discuss services with
9 clients through email and other communications; (d) to post information to the website
10 and social media accounts of the business. Therefore, I believe that in addition to seizing
11 the digital devices to conduct a search of their contents as set forth herein, there is
12 probable cause to seize those digital devices as instrumentalities of the criminal activity.

13 32. If, after conducting its examination, law enforcement personnel determine
14 that any digital device is any instrumentality of the criminal offenses referenced above,
15 the government may retain that device during the pendency of the case as necessary to,
16 among other things, preserve the instrumentality evidence for trial, ensure the chain of
17 custody, and litigate the issue of forfeiture. If law enforcement personnel determine that
18 a device was not an instrumentality of the criminal offenses referenced above, it shall be
19 returned to the person/entity from whom it was seized within 90 days of the issuance of
20 the warrant, unless the government seeks and obtains authorization from the Court for its
21 retention.

22 **PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

23 33. Because of the nature of the evidence that I am attempting to obtain and the
24 nature of the investigation, I have not made any prior efforts to obtain the evidence based
25 on the consent of any party who may have authority to consent. I believe, based upon the
26 nature of the investigation and the information I have received, that if VALDEZ becomes
27 aware of the search warrant, he may attempt to destroy any potential evidence, whether
28

1 digital or non-digital, thereby hindering law enforcement agents from the furtherance of
2 the criminal investigation.

3 **RISK OF DESTRUCTION OF EVIDENCE**

4 34. I know, based on my training and experience, that digital information can
5 be very fragile and easily destroyed. Digital information can also be easily encrypted or
6 obfuscated such that review of the evidence would be extremely difficult, and in some
7 cases impossible. I do not know whether, in the instant case, VALDEZ used encryption
8 on the computer systems he utilizes to engage in his crimes. If an encrypted computer is
9 either powered off, or if the user has not entered the encryption password and logged onto
10 the computer, it is likely that any information contained on the computer will be
11 impossible to decipher. If the computer is powered on, however, and the user is already
12 logged onto the computer, there is a much greater chance that the digital information can
13 be extracted from the computer. This is because when the computer is on and in use, the
14 password has already been entered and the data on the computer is accessible. However,
15 giving the owner of the computer time to activate a digital security measure, pull the
16 power cord from the computer, or even log off of the computer, could result in a loss of
17 digital information that could otherwise have been extracted from the computer.

18 **REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF**
19 **TARGET COMPUTERS AND OTHER DIGITAL DEVICES**

20 35. In most cases, a thorough search of a premise for information that might be
21 stored on storage media often requires the seizure of the physical storage media and later
22 off-site review consistent with the warrant. In lieu of removing storage media from the
23 premises, it is sometimes possible to make an image copy of storage media. Generally
24 speaking, imaging is the taking of a complete electronic picture of the computer's data,
25 including all hidden sectors and deleted files. Either seizure or imaging is often
26 necessary to ensure the accuracy and completeness of data recorded on the storage media,
27 and to prevent the loss of the data either from accidental or intentional destruction. This
28 is true because of the following:

1 a. *The time required for an examination.* As noted above, not all
2 evidence takes the form of documents and files that can be easily viewed on site.
3 Analyzing evidence of how a computer has been used, what it has been used for,
4 and who has used it requires considerable time, and taking that much time on
5 premises could be unreasonable. As explained above, because the warrant calls for
6 forensic electronic evidence, it is exceedingly likely that it will be necessary to
7 thoroughly examine storage media to obtain evidence. Storage media can store a
large volume of information. Reviewing that information for things described in
the warrant can take weeks or months, depending on the volume of data stored,
and would be impractical and invasive to attempt on-site.

8 b. *Technical requirements.* Computers can be configured in several
9 different ways, featuring a variety of different operating systems, application
10 software, and configurations. Therefore, searching them sometimes requires tools
11 or knowledge that might not be present on the search site. The vast array of
12 computer hardware and software available makes it difficult to know before a
13 search what tools or knowledge will be required to analyze the system and its data
14 on the Premises. However, taking the storage media off-site and reviewing it in a
controlled environment will allow its examination with the proper tools and
knowledge.

15 c. *Variety of forms of electronic media.* Records sought under this
16 warrant could be stored in a variety of storage media formats that may require off-
17 site reviewing with specialized forensic tools.

18 36. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
19 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,
20 or otherwise copying digital devices or other electronic storage media that reasonably
21 appear capable of containing some or all of the data or items that fall within the scope of
22 Attachment B to the application seeking authorization to search the PREMISES, and will
23 specifically authorize a later review of the media or information consistent with that
24 warrant.

25 37. Consistent with the above, I am requesting the authority to seize and/or
26 obtain a forensic image of digital devices or other electronic storage media that
27 reasonably appear capable of containing data or items that fall within the scope of
28 Attachment B to the application seeking authorization to search the PREMISES, and to

1 conduct off-site searches of the digital devices or other electronic storage media and/or
2 forensic images, using the following procedures:

- 3 a. Upon securing the physical search site, the search team will conduct an
4 initial review of any digital devices or other electronic storage media
5 located at the PREMISES described in Attachment A that are capable of
6 containing data or items that fall within the scope of Attachment B to this
7 Affidavit, to determine if it is possible to secure the data contained on these
8 devices onsite in a reasonable amount of time and without jeopardizing the
9 ability to accurately preserve the data.
- 10 b. In order to examine the electronically stored information ("ESI") in a
11 forensically sound manner, law enforcement personnel with appropriate
12 expertise will attempt to produce a complete forensic image, if possible and
13 appropriate, of any digital device or other electronic storage media that is
14 capable of containing data or items that fall within the scope of Attachment
15 B.
- 16 c. A forensic image may be created of either a physical drive or a logical
17 drive. A physical drive is the actual physical hard drive that may be found
18 in a typical computer. When law enforcement creates a forensic image of a
19 physical drive, the image will contain every bit and byte on the physical
20 drive. A logical drive, also known as a partition, is a dedicated area on a
21 physical drive that may have a drive letter assigned (for example the c: and
22 d: drives on a computer that actually contains only one physical hard drive).
23 Therefore, creating an image of a logical drive does not include every bit
24 and byte on the physical drive. Law enforcement will only create an image
25 of physical or logical drives physically present on or within the subject
26 device. Creating an image of the devices located at the search location
27 described in Attachment B will not result in access to any data physically
28 located elsewhere. However, digital devices or other electronic storage
media at the search location described in Attachment A that have
previously connected to devices at other locations may contain data from
those other locations.
- d. In addition to creating an image of a physical or logical drive from a digital
device or other electronic storage media, law enforcement may attempt to
create an image of the random access memory ("RAM") of a digital device.
Agents may only create an image of a digital device's RAM if the computer
is powered on at the time of the search. This is because RAM is only active
when the device is in operation. Any data contained in the RAM will be

1 lost when the computer is powered off. A computer's RAM may contain
2 evidence related to who else is logged onto the computer (even remotely),
3 open connections that might indicate a program is waiting for commands,
4 passwords for encryption programs, hardware and software settings, maps
5 of recent files and applications accessed, and information related to what
6 communication vendors have recently been utilized on the device (i.e.
7 instant messaging services, e-mail services, social networking sites, etc.).
8 In addition, RAM may contain encryption keys necessary to access other
9 elements of the subject device.

- 10 e. If based on their training and experience, and the resources available to
11 them at the search site, the search team determines it is not practical to
12 make an on-site image within a reasonable amount of time and without
13 jeopardizing the ability to accurately preserve the data, then the digital
14 devices or other electronic storage media will be seized and transported to
15 an appropriate law enforcement laboratory to be forensically imaged and
16 reviewed.
- 17 f. Searching the forensic images for the items described in Attachment B may
18 require a range of data analysis techniques. In some cases, it is possible for
19 agents and analysts to conduct carefully targeted searches that can locate
20 evidence without requiring a time-consuming manual search through
21 unrelated materials that may be commingled with criminal evidence. In
22 other cases, however, such techniques may not yield the evidence described
23 in the warrant, and law enforcement may need to conduct more extensive
24 searches to locate evidence that falls within the scope of the warrant. The
25 search techniques that will be used will be only those methodologies,
26 techniques and protocols as may reasonably be expected to find, identify,
27 segregate and/or duplicate the items authorized to be seized pursuant to
28 Attachment B to this affidavit. Those techniques, however, may
necessarily expose many or all parts of a hard drive to human inspection in
order to determine whether it contains evidence described by the warrant.
- g. These methodologies, techniques and protocols may include the use of a
"hash value" library to exclude normal operating system files that do not
need to be further searched. Agents may utilize hash values to exclude
certain known files, such as the operating system and other routine
software, from the search results. However, because the evidence I am
seeking does not have particular known hash values, agents will not be able

1 to use any type of hash value library to locate the items identified in
2 Attachment B.


3 **CONCLUSION**

4 40. Based upon the evidence set forth herein, I respectfully submit that there is
5 probable cause to believe that VALDEZ committed the evasion of the assessment of
6 personal taxes for 2017 in violation of Title 26, United States Code, Section 7201. I also
7 respectfully submit that there is probable cause to believe that VALDEZ willfully aided
8 or assisted in the preparation of false tax returns for the year 2017, in violation of
9 Title 26, United States Code, Section 7206(2). Moreover, I believe that there is probable
10 cause to believe that evidence, fruits, and instrumentalities of these crimes, more fully
11 described in Attachment B, are currently located at the PREMISES more fully described
12 in Attachment A, as well as on and in any digital devices or other electronic storage
13 media found at or within the PREMISES. I therefore request that the Court issue a
14 Warrant authorizing the search of the PREMISES, as well as any digital devices and
15 electronic storage media located at the PREMISES, for the items described in Attachment
16 B and the seizure of any such items found herein.

17
18 Respectfully submitted,

19
20 
21 CHRISTIAN D. MARTIN, Affiant
22 IRS Criminal Investigation

23 The above-named agent provided a sworn statement attesting to the truth of the
24 contents of the foregoing affidavit by telephone on the 1st day of February, 2019.

25
26 
27 J. RICHARD CREATURA
28 United States Magistrate Judge